U.S. FOREIGN POLICY AGENDA

VOLUME 6 AN ELECTRONIC JOURNAL OF THE U.S. DEPARTMENT OF STATE NUMBER 3

Threat Assessment, Countermeasures and Policy

November 2001

On September the 11th, enemies of freedom committed an act of war against our country. Americans have known wars — but for the past 136 years, they have been wars on foreign soil, except for one Sunday in 1941. Americans have known the casualties of war — but not at the center of a great city on a peaceful morning. Americans have known surprise attacks — but never before on thousands of civilians. All of this was brought upon us in a single day — and night fell on a different world, a world where freedom itself is under attack...

This is not, however, just America's fight. And what is at stake is not just America's freedom. This is the world's fight. This is civilization's fight. This is the fight of all who believe in progress and pluralism, tolerance and freedom.

We ask every nation to join us. We will ask, and we will need, the help of police forces, intelligence services, and banking systems around the world. The United States is grateful that many nations and many international organizations have already responded — with sympathy and with support. Nations from Latin America, to Asia, to Africa, to Europe, to the Islamic world. Perhaps the NATO Charter reflects best the attitude of the world: An attack on one is an attack on all.

The civilized world is rallying to America's side. They understand that if this terror goes unpunished, their own cities, their own citizens may be next. Terror, unanswered, cannot only bring down buildings, it can threaten the stability of legitimate governments. We're not going to allow it...

The course is not known, yet its outcome is certain. Freedom and fear, justice and cruelty, have always been at war, and we know that God is not neutral between them.

George W. Bush
President of the United States of America

Editor's Note: This 20th issue of U.S. Foreign Policy Agenda — planned well before the tragic events of September 11th in New York, the Washington, D.C. area, and Pennsylvania — explores major themes in international terrorism and its increasingly violent nature through a series of articles, fact sheets and references from experts within the United States Government and from the academic and private sectors.

U.S. FOREIGN POLICY
A G E N D A

An Electronic Journal of the
U.S. Department of State

TERRORISM: THREAT ASSESSMENT, COUNTERMEASURES AND POLICY

CONTENTS

PREFACE 2

By George W. Bush
President of the United States of America

FOCUS

SEIZING THE MOMENT 5

By Colin L. Powell
Secretary of State, United States of America

TERRORISM: U.S. POLICIES AND COUNTERTERRORISM MEASURES 7

By Ambassador Francis X. Taylor
Office of the Coordinator for Counterterrorism, U.S. Department of State

THE INSTRUMENTS OF COUNTERTERRORISM 10

By Paul R. Pillar
National Intelligence Officer for Near East and South Asia; National Intelligence Council, Central Intelligence Agency

PROTECTING AMERICA AGAINST CYBERTERRORISM 14

By Paul Rodgers
Assistant Unit Chief, Outreach and Field Support Unit, National Infrastructure Protection Center
Federal Bureau of Investigation

MANY COUNTRIES BENEFIT FROM U.S. ANTITERRORISM TRAINING 18

By Alan O. Bigler
Director, Antiterrorism Assistance Program, Bureau of Diplomatic Security, U.S. Department of State

COMMENTARY

TERRORISM AND COUNTERTERRORISM AFTER SEPTEMBER 11TH 22

By Bruce Hoffman
Vice President, External Affairs Director, RAND Corporation Washington Office

ANTHRAX AND MASS-CASUALTY TERRORISM: WHAT IS THE BIOTERRORIST THREAT AFTER SEPTEMBER 11TH 25

By Jason Pate
Senior Research Associate and Manager, WMD Terrorism Database, Monterey Institute of International Studies

BRINGING TERRORISTS TO JUSTICE UNDER THE RULE OF LAW 29

By Peter Raven-Hansen
Glen Earl Weston Research Professor of Law, The George Washington University Law School

FACT SHEETS

INTERNATIONAL TERRORISM: AMERICAN HOSTAGES 32

STATE-SPONSORED TERRORISM AND FOREIGN TERRORIST ORGANIZATIONS 34

A GUIDE TO ADDITIONAL READING

TERRORISM: THREAT ASSESSMENT, COUNTERMEASURES AND U.S. POLICY ARTICLE ALERT 36

Abstracts of recent articles

TERRORISM: THREAT ASSESSMENT, COUNTERMEASURES AND U.S. POLICY BIBLIOGRAPHY 37

Spotlighting other views

TERRORISM: THREAT ASSESSMENT, COUNTERMEASURES AND U.S. POLICY KEY INTERNET SITES 38

Internet links to resources on related issues

U.S. FOREIGN POLICY AGENDA

AN ELECTRONIC JOURNAL OF THE U.S. DEPARTMENT OF STATE — VOLUME 6 • NUMBER 3 • NOVEMBER 2001

Editor, U.S. Foreign Policy Agenda
Political Security — IIP/T/PS
U.S. Department of State
301 4th Street, S.W.
Washington, D.C. 20547
United States of America
E-mail: ejforpol@pd.state.gov

Please note that this issue of U.S. FOREIGN POLICY AGENDA can be located on the Office of International Information Programs' International Home Page on the World Wide Web at "http://www.usinfo.state.gov/journals/itps/1101/ijpe/ijpe1101.htm".

SEIZING THE MOMENT

By Secretary of State Colin L. Powell

"International terrorism poses a multidimensional threat. Our coalition must use every tool of statecraft to defeat it," says Secretary of State Colin L. Powell. "This will be a long, hard campaign, measured in years and fought on many fronts. For such an effort, our coalition will have the flexibility to evolve. And the very process of participating in this great global campaign against terrorism may well open the door for us to strengthen or reshape international relationships and expand or establish areas of cooperation."

The mass murders that were committed on September 11 under the direction of Osama bin Laden and his al-Qaida network have united the world against international terrorism. Some 80 countries lost citizens in the attacks. From our shared grief and shared resolve can come new opportunities not only to defeat terrorism, but also to work with other nations on a range of important issues of global concern.

A host of countries and international organizations have answered President Bush's call for a worldwide coalition to combat terrorism — among them NATO, the European Union, the Organization of American States, the Association of Southeast Asian Nations, the Organization of African Unity, the Arab League, the Organization of the Islamic Conference, and the U.N. General Assembly and Security Council. Indeed, the Security Council unanimously adopted an historic resolution obliging all 189 U.N. member states to stop terrorist travel, money flows, planning and other support, and to cooperate in bringing terrorists to justice.

International terrorism poses a multidimensional threat. Our coalition must use every tool of statecraft to defeat it. Some countries will take part in the military response against those involved in the atrocities of September 11. Others, while not participating directly in military action, will provide logistical support or access to bases and staging areas or overflight rights. And many will contribute to humanitarian efforts to help the millions of innocent Afghans who have suffered under the Taliban regime — a regime which seems to care more about Osama bin Laden and his terrorists than its own starving citizens. Coalition members also will work to disrupt and destroy terrorist networks by sharing intelligence and other critical information, cooperating in law enforcement, and cutting off terrorists' financial lifelines.

This will be a long, hard campaign, measured in years and fought on many fronts. For such an effort, our coalition will have the flexibility to evolve.

And the very process of participating in this great global campaign against terrorism may well open the door for us to strengthen or reshape international relationships and expand or establish areas of cooperation.

Already, our alliances in Europe, Asia and the Western Hemisphere have been reinvigorated by invocations of the collective defense provisions of the NATO, ANZUS and Rio Treaties.

Russian President Vladimir Putin's reaction to September 11 marked the beginning of a new period in our bilateral relationship, one in which a new spirit of cooperation on counterterrorism may also make many of the tough issues on the agenda more resolvable. Indeed, in the wake of 11 September, it has become clear that not only is the Cold War over, but the post-Cold War period is also over.

China has also contributed meaningfully to this unprecedented global effort. I am confident that as we advance our counterterrorism cooperation with China

we will be in a stronger position to sustain meaningful consultations with the leadership in Beijing on other subjects of importance to us.

We have also seized opportunities to improve our relations with Pakistan and India. President Musharaff of Pakistan made the strategic decision to end his government's support of the Taliban. As a result of the actions taken by Pakistan in support of our campaign, we can see the beginning of a strengthened relationship that will grow and thrive in the years ahead.

Well before September 11, President Bush made it clear that putting our relationship with India on a higher plane is one of his highest priorities. With the strong support we have received from the Indian government since September 11, we are seizing the opportunity to accelerate the pace of change.

Our improved relations with these two South Asian rivals may now present an opportunity for both countries to explore new ways of thinking about stability on the Subcontinent.

The millions of our fellow Americans of the Islamic faith, and the ten Muslim nations who lost citizens in the September 11 attacks, need no convincing that the killers and their accomplices pervert Islam when they use it to justify their appalling crimes. Out of a deep sense of shared humanity, and a chilling appreciation of common vulnerability to terrorism, we see new scope to strengthen our relations with the Islamic world.

In this global campaign, the United States welcomes the help of any country or party that is genuinely prepared to work with us, but we will not relax our standards and we will continue to advance our fundamental interests in human rights, accountable government, free markets, non-proliferation and conflict resolution, for we believe that a world of democracy, opportunity, and stability is a world in which terrorism cannot thrive.

Throughout the campaign against international terrorism, the dedicated men and women of the State Department at our posts abroad and here in Washington will be on the front lines just as surely as those who wear the uniform.

We will not let terrorism hijack American foreign policy. The President has urged the American people to get back to the business of their daily lives. So too, the United States will continue to pursue a full international agenda — from promoting good governance to cooperating with other countries to stem the HIV/AIDS pandemic, establish a post-Cold War strategic framework, launch a new trade round, and foster peace in the Middle East.

Terrorism has cast a shadow across the globe. But the global resolve to defeat it has never been greater and the prospects for international cooperation across a broad range of issues has never been brighter. As President Bush said the other day when he visited the State Department: "Out of this evil will come good. Through our tears we see opportunities to make the world better for generations to come. And we will seize them." ◉

TERRORISM: U.S. POLICIES AND COUNTERTERRORISM MEASURES

By Ambassador Francis X. Taylor
Coordinator for Counterterrorism, U.S. Department of State

"The war we are waging will be a long struggle with many dimensions," says Ambassador Francis X. Taylor, the State Department's Coordinator for Counterterrorism. "Our goal is to eliminate the international terrorist threat to people, installations, and other interests."

September 11, 2001 is a day that will redefine history. Before the tragic events of that date occurred, articles appeared in journals and newspapers accusing the U.S. Government of overstating the terrorist threat. This is no longer the case. The terrorist attacks that were launched on that day in New York, Virginia, and Pennsylvania claimed victims from some 88 nations, from our close neighbors Canada and Mexico to countries as far away as Australia and Zimbabwe, and in large numbers from India and Pakistan. For many countries, including the United States, Britain, Germany, and Switzerland, the horrors of September 11 claimed the most lives of any terrorist incident in their history. For the United States, it was the bloodiest day in America since the 1862 Civil War Battle of Antietam.

The attacks may have been conceived as a blow against America, but in reality they were attacks against all of humanity and civilization itself.

The war we are waging will be a long struggle with many dimensions. Our goal is to eliminate the international terrorist threat to people, installations, and other interests. We will do this by:

- Smoking out terrorists from their hiding places,
- Draining the swamp where terrorists find safe haven,
- Pressuring states to stop supporting terrorism,
- Preventing planned terrorist attacks, and
- Bolstering the capabilities of our friends and allies to combat terrorism.

The nations of the world are banding together to eliminate the terrorism scourge. Numerous multilateral organizations have issued declarations of support, including the United Nations, the European Union, the Organization of American States, the Organization for African Unity, the Organization of the Islamic Conference, and the Asia-Pacific Economic Cooperation forum, and many others have expressed their strong solidarity.

I recently traveled to Brussels where I met with the North Atlantic Council. I made the case that the al-Qaida organization led by Osama bin Laden was responsible for what happened on the 11th of September. I traced the history of this organization, its recent activities, and the events that occurred just prior to and just after the 11th.

In response, NATO Secretary General Lord Robertson stated that the facts contained in the briefing were "clear and compelling" and point "conclusively to an al-Qaida role in the attacks." As a result of the briefing, NATO concluded that the attacks were directed from abroad and will "therefore be regarded as an action covered by Article V of the Washington Treaty, which states that an armed attack on one or more of the allies in Europe or North America shall be considered an attack against them all." This was the first time Article V was invoked in the history of the NATO alliance.

NATO allies have agreed to provide the United States with the wide range of assistance that we had requested. This includes unlimited use of their airspace, base

facilities, seaports, logistics, extra security for U.S. forces in Europe, intelligence sharing, and early warning aircraft. AWACS surveillance planes belonging to NATO are currently patrolling the skies over America as a result of the Article V invocation. The Organization of American States invoked the Rio Treaty, which also covers collective self-defense. OAS foreign ministers, meeting in Lima, Peru on the day of the attacks, were the first to condemn them.

The Organization of the Islamic Conference — the most important and comprehensive grouping of Muslim states, 56 in all — strongly condemned the savage September 11 attacks and unequivocally declared that terrorism is never sanctioned by Islam. We believe the face of terror is not the true face of Islam. Terrorism is a perversion of religion, and those who hijacked our airplanes on September 11 also hijacked the faith they claim.

Other nations, great and small, have made pledges and contributions to what is a global response to a global attack. We have received numerous offers of diplomatic, political, police, intelligence, and military support. We have what amounts to a coalition of coalitions, with some nations forging ahead to deny terrorists access to banking systems, for example, and other nations more active in other areas. Individual members are dedicated and are holding steady. Our challenge will be to hold the coalitions together until the campaign is successful.

FORGING THE TOOLS TO FIGHT TERROR

This campaign will be unlike others we have fought. The battles are as likely to be fought in small conference rooms among bankers, at border crossing points, or in forensic laboratories as over the skies of some hostile power. Our victories will be counted in the drying up of financing, the withering of political support, the rounding up of terrorist cells — not in the conquest of foreign land.

TERRORIST FUNDING

The September 11 terrorists apparently had enough money to make their preparations many months, if not years, in advance. Funding is a critical element in recruiting supporters and launching large-scale terrorist operations. We need to dry up terrorist fundraising and money transfers.

The first shot in the war against terrorism was fired on September 24 when President Bush signed executive order 13224. This shot froze the assets of 27 terrorists, terrorist organizations, and terrorist financiers associated with al-Qaida and blocks U.S. transactions with such persons or entities. The Executive Order was later amended to include 39 additional names of persons and organizations known to conduct or financially support terrorism. In addition, the assets of all 22 of the FBI's Most Wanted Terrorists are now subject to this blocking order. Additional names will be added in the months ahead.

A previous Executive Order, in effect since 1995 and renewed each year since, includes such groups as Hizballah and HAMAS, as well as al-Qaida, that represent a terrorist threat to the Middle East peace negotiations.

On September 28 the U.N. Security Council unanimously adopted resolution 1373, which is binding on all states under international law. This resolution goes to the heart of how terrorism operates. It obliges all member states to deny financing, support, and safe haven to terrorists. It will also expand information sharing among U.N. members to combat international terrorism. A Security Council follow-up mechanism has been set up to monitor compliance on a continuous basis.

This effort has already yielded results. The United States has frozen some $4 million and is reviewing many other accounts. We have received reports of millions of additional dollars being frozen around the world. Other nations are still seeking to identify terrorist assets that they have pledged to block. In all, 111 nations — more than half the world — have acted to choke off the oxygen of money for terrorists, and this is only the beginning.

Another important tool in countering terrorist fundraising is formally designating groups as Foreign Terrorist Organizations, or FTOs. Designation of FTOs makes it a criminal offense for persons subject to U.S. jurisdiction to knowingly contribute funds or other material support to such groups. U.S. law also

allows freezing of the groups' assets and denial of visas for their leaders and other members. Secretary of State Colin Powell designated 28 such groups, including al-Qaida, in early October.

Using tools like these, we have urged other countries to tighten up their own laws and regulations to curb terrorist fundraising and money transfers. Great Britain already has done so, and countries such as Canada, Greece, India, and the Philippines have new laws or proposed counterterrorism legislation in various stages of consideration.

In addition, the administration is making ratification of the 12 U.N. conventions against terrorism a high priority. These cover a range of activities, such as hijacking, hostage taking, bombing, and terrorism financing. The conventions form a strong legal framework for fighting terrorism.

OTHER MEASURES

There are a number of other tools that we have been using to counter terrorism, and we are sharpening and improving them in this new struggle.

We are utilizing training-related programs to help combat terrorism overseas and thus help protect Americans living and traveling abroad. The State Department's Antiterrorism Training Assistance (ATA) program in which we train foreign security and law enforcement officials is a pillar of this effort. The program not only provides training but also helps promote our policies and improve our contacts with foreign officials to achieve our counterterrorism goals. We have trained more than 20,000 officials from over 100 countries to date. We are hoping for additional funding for the ATA program in the wake of the September 11 attacks to permit us to accelerate the pace of this training.

We also have developed a Terrorist Interdiction Program (TIP), which utilizes sophisticated computer data base systems and improved communications to help identify potential terrorists who try to cross international borders. This program will be most effective in countries that are major transportation hubs.

The Department's contribution to the interagency counterterrorism research and development program, the Technical Support Working Group, also helps to make advances in explosives detection and other areas and bolster our cooperative R&D efforts with other key allies.

We have proposed increasing our "Rewards for Justice" program, which pays up to $5 million for information that prevents a terrorist attack or results in the arrest of a terrorist. This important program saves lives and puts terrorists behind bars.

Many challenges lie ahead. Maintaining the international coalition will be one. However, in the months that have elapsed since these nations proclaimed their solidarity against terrorism, the coalition has gotten stronger. Another challenge will be to counter the notion held in some quarters that Osama bin Laden is some type of hero and that the United States is somehow the aggressor. I believe, that, through active public diplomacy, we can effectively convey the message that bin Laden is evil, and his actions are a manifestation of evil. Moreover, the United States has no designs on foreign real estate. We are not an invading force. But we will forcefully attack the terrorist network that represents a threat to us all.

The horrific events of September 11 require a broad based, long-term strategic campaign, in concert with the nations of the world that abhor terrorism. Together we will root out and bring to justice those that use terrorism. We are in for a long haul. As President Bush has told the world: "Whether we bring our enemies to justice, or bring justice to our enemies, justice will be done."

THE INSTRUMENTS OF COUNTERTERRORISM

By Paul R. Pillar
National Intelligence Officer for Near East and South Asia
National Intelligence Council, Central Intelligence Agency

Counterterrorism, which involves an array of activities that exceed the term "counterterrorism," includes effective use of diplomacy, law enforcement, financial controls, military power, and intelligence gathering, says Paul R. Pillar, a national intelligence officer for the Near East and South Asia with the National Intelligence Council. "Every counterterrorist instrument is difficult to use. Using them well together is even more difficult. But using them all is critical in the fight against terrorism."

Every tool used in the fight against terrorism has something to contribute, but also significant limits to what it can accomplish. Thus, counterterrorism requires using all the tools available, because no one of them can do the job. Just as terrorism itself is multifaceted, so too must be the campaign against it.

Counterterrorism involves far more activities than those that bear the "counterterrorist" label. Even before the attacks of 11 September 2001 made the subject a seemingly all-encompassing concern for the United States, it involved the efforts of many different departments and agencies. Counterterrorism includes diplomacy designed to harmonize the efforts of foreign governments on the subject. It includes the investigative work of numerous law enforcement agencies and the related legal work of prosecuting terrorist crimes. It involves measures by financial regulatory bodies to interrupt terrorist funding. As the allied military operations begun over Afghanistan in October 2001 remind us, it, at times, includes the use of armed force. Information gathering by intelligence agencies is another major part of counterterrorism. And all of these functions aimed at actively countering terrorist operations are in addition to the many defensive measures, taken by the private sector as well as by various levels of government, designed to protect against terrorist attacks.

DIPLOMACY

Diplomacy is critical to combating modern international terrorism which, in many respects, knows no boundaries. Terrorist groups have increasingly spread their reach around the globe. Combating a terrorist network like the one that includes Osama bin Laden's al-Qaida group requires the cooperative efforts of many countries because the network operates in many countries. Effective counterterrorist diplomacy is the glue needed to hold these efforts into a coherent whole rather than being merely disjointed parts. The building of a counterterrorist coalition following the attacks of 11 September is only the most recent and conspicuous demonstration that the United States needs the help of foreign partners in countering even those threats directed specifically against the United States.

Counterterrorist diplomacy is not just the responsibility of professional diplomats in foreign ministries. Officials performing other specialized, and counterterrorist-related, functions have to cooperate extensively with foreign counterparts to do their jobs. Regulatory agencies responsible for the security of civil aviation and other modes of transportation, for example, have to perform what is, in effect, a diplomatic function to accomplish the necessary coordination where their security systems intersect with those of other countries. Customs and immigration officials must do the same.

Most of this specialized cooperation is bilateral, but multilateral diplomacy also has contributions to make. It can provide broad sanction for measures that would have less legitimacy if taken by an individual state. The United Nations Security Council has done so, for

example, with resolutions (beginning with Resolution 1267 in 1999) pertaining to the Taliban's support to terrorism based in Afghanistan. Multilateral diplomacy — including resolutions of the U.N. General Assembly and a dozen international conventions on terrorism — also strengthens an international norm against terrorism. Some of those conventions, such as ones dealing with hijacking of aircraft, also provide a basis for practical cooperation on matters where national jurisdictions may overlap.

The limitations of diplomacy as a counterterrorist tool are obvious. Terrorists do not change their behavior in direct response to a treaty or U.N. resolution. But diplomacy supports all of the other tools, whether by broadening the moral force behind them or providing an international legal framework for their use.

CRIMINAL LAW

The prosecution of individual terrorists in criminal courts has been one of the most heavily relied upon counterterrorist tools. The United States has placed particular emphasis on it, with the bringing of terrorists to justice for their crimes being a longstanding tenet of U.S. counterterrorist policy. Non-U.S. courts have also played significant roles. A Scottish court sitting in the Netherlands was used to try two suspects accused of bombing Pan Am flight 103 in 1988.

Use of the criminal justice system can help reduce terrorism in several ways. Imprisoning a terrorist for life (or executing him) obviously prevents him from conducting any more attacks. The prospect of being caught and punished may deter other terrorists from attacking in the first place. Even if not deterred, the movements of terrorists still at large can be impeded by the knowledge that they are wanted men. The drama and publicity of a criminal trial may also help to sustain public support for counterterrorism, demonstrate a government's resolve to go after terrorists, and encourage other governments to do the same.

A limitation of applying the criminal justice system to terrorism is that the prospect of being caught and punished does not deter some terrorists. That prospect is obviously irrelevant to suicide bombers, and perhaps also to other low-level operatives who feel a comparable level of commitment and desperation. High-level terrorist leaders — who typically stay farther removed from the scene of the crime and are more difficult to catch — may care little about whether the underlings are caught.

Prosecuting a terrorist also poses the practical difficulty of assembling sufficient legally admissible evidence to convict him. At least in U.S. courts, that is a higher standard than acquiring enough information to be fairly sure, from an intelligence or policy perspective, that someone is a terrorist. Direct evidence of the decisions or orders issued by terrorist leaders is particularly hard to come by. The physically dispersed planning and decision making of international terrorist groups means many of the actions leading to a terrorist attack were taken outside the country where the attack occurs and outside the jurisdiction of the lead investigators.

The need for international cooperation in applying criminal law to terrorists is obvious. It involves not only acquisition of evidence for use in court but also the extradition or rendition of fugitives to stand trial in the country where they are charged.

FINANCIAL CONTROLS

The funding that evidently made it possible for the perpetrators of the attacks in September to train and travel as they prepared for their operation has highlighted efforts to interdict terrorist money. The United States uses two types of financial controls to combat terrorism: the freezing of assets belonging to individual terrorists, terrorist groups, and state sponsors; and the prohibition of material support to terrorists. Money is also the subject of the most recent multilateral treaty on terrorism: the Convention on the Suppression of the Financing of Terrorism, which was opened for signature in January 2000.

Cutting off terrorists' funding faces two major challenges. One is that — notwithstanding the importance of financial backing to the September hijackers — most terrorism does not require large-scale financing. Less money is involved than in illegal narcotics, arms trafficking, and some other transnational criminal activities. The other challenge is that the flow of terrorist money is extremely difficult to

track. False account names, the use of financial intermediaries, and commingling of funds for legitimate and illegitimate purposes are the rule. Much money gets moved through informal arrangements outside any formal banking system.

Despite these challenges, more could be accomplished to impede terrorists' financial operations. The Treasury Department's Office of Foreign Assets Control (OFAC) provides focus and direction for U.S. efforts on this subject, but most of the financial activity, even of groups targeting the United States, takes place outside U.S. jurisdiction. The creation in other governments of offices similar to OFAC and the close cooperation of such offices would make a further dent in terrorists' financial activity.

MILITARY FORCE

Modern, precision-guided munitions have made armed force a less blunt and more useful counterterrorist instrument, but one whose use is still appropriately rare. Several countries have used military force with varying degrees of success over the last three decades to rescue hostages. More recently the military instrument has been employed to retaliate against terrorist attacks. The United States has used its armed forces for retaliation following terrorist attacks by Libya in 1986, Iraq in 1993, and Osama bin Laden in 1998.

A military strike is the most forceful possible counterterrorist action and thus the most dramatic demonstration of determination to defeat terrorists. The major limitation of military force is that terrorist assets, unlike conventional military assets, do not present large, fixed targets that can readily be destroyed. With the terrorist threat now coming much more from groups than from states, there are even fewer targets to strike, either to damage terrorist capabilities or to deter future terrorism.

The U.S. and British military operations begun in Afghanistan in October go beyond any previous counterterrorist use of military force, in that they constitute not just retaliation but an effort to clean out the prime source and safe haven of a terrorist network. In their goal and scale, they have the potential for having a substantially greater effect on terrorism than any previous use of armed force. Success in Afghanistan will depend on political as well as military chapters of that country's history yet to be written. Even with success in Afghanistan, however, the military operations there do not directly touch the portions of the al-Qaida network that reside elsewhere, and, thus, must be part of a broader counterterrorist effort that does address those portions.

INTELLIGENCE

The collection and analysis of intelligence is the least visible but in some ways the most important counterterrorist tool, and is rightly thought of as the "first line of defense" against terrorism. But this instrument also has its limitations, chief of which is that the type of very specific, tactical intelligence required to thwart terrorist plots is rare. That kind of actionable information is difficult to collect because it requires penetration of groups that are small, suspicious of outsiders, and very careful about their operational security.

Most intelligence about terrorist groups is fragmentary, ambiguous, and often of doubtful credibility. Analysis is thus almost as much of a challenge as collection. The contribution of intelligence is not so much to provide coherent pictures of impending terrorist operations but rather a more strategic sense of which groups pose the greatest threats, which times and which regions present the greatest dangers, and what sorts of targets and tactics are most likely to be used.

The limitations of counterterrorist intelligence mean it should not be relied upon as a foolproof indicator of where threats do and do not exist. But the guidance it provides in managing the risks from terrorism is invaluable, from decisions on site security to broader policy on allocation of counterterrorist resources, as well as being essential to the functioning of all the other counterterrorist instruments.

PUTTING IT ALL TOGETHER

The instruments discussed here must be well coordinated. Used together wisely, they produce a whole that is greater than the sum of the parts. If not well coordinated, they can work at cross-purposes.

Enforcement of criminal law may get in the way of intelligence collection, for example, and military action could disrupt either law enforcement or intelligence gathering.

The United States accomplishes day-to-day coordination through sub-cabinet committees, cross-assignment of personnel, and other formal and informal mechanisms centered in the National Security Council and involving the Departments of State, Defense, Justice, and Treasury, the intelligence agencies, and other elements. The best arrangements for coordinating counterterrorism will vary from one government to another, but effective coordination should reflect three principles. One is that all of the relevant ministries or agencies — including those responsible for military affairs, internal security, intelligence, and foreign affairs — need to be involved. Second, leadership should come from the center, such as a cabinet office or equivalent to the U.S. National Security Council. And third, the various offices involved need to develop everyday habits of working together that will become second nature and pay off during a crisis.

Every counterterrorist instrument is difficult to use. Using them well together is even more difficult. But using them all is critical in the fight against terrorism.

PROTECTING AMERICA AGAINST CYBERTERRORISM

By Paul Rodgers
Assistant Unit Chief, Outreach and Field Support Unit, National Infrastructure Protection Center
Federal Bureau of Investigation

"Although the means and ends have evolved throughout history, the central elements of terrorism — fear, panic, violence and disruption — have changed little," says Paul Rodgers of the National Infrastructure Protection Center at the Federal Bureau of Investigation. "Today, tremendous destructive potential fits into easily transported packages (bombs, nerve gas and biological agents), and the computers that are connected to the Internet can be attacked from any point on the globe.... The need for the heightened security of critical operations has grown markedly in recent years as a result of the escalation in the use of information technology to improve performance, increased competitive pressures from deregulation and globalization, and the concentration of operations in a smaller number of facilities to decrease costs, with the resulting reduction in redundancy and reserve capacity."

THE WAR ON TERRORISM

With the destruction of the World Trade Center Towers and the attack on the Pentagon September 11th and the continuing anthrax attacks, the United States has entered a new age of terrorism that targets both civilians and soldiers in a war with no rules and no clear ending. There has been a steady progression toward this point by such events as the 1988 bombing of Pan Am Flight 103 over Lockerbie, Scotland, the 1989 Hannover Hackers case, the 1994 Citibank fraud case, and the 1995 Oklahoma City bombing.

Although the means and ends have evolved throughout history, the central elements of terrorism — fear, panic, violence and disruption — have changed little. As the world enters the 21st Century, terrorism remains a vexing problem — an anachronistic fixture of human relations as paradoxically human and inhuman in the Third Millennium as it was before the dawn of recorded history. While terrorists once generally used acts of terrorism as a means to publicize their causes, the operational objectives in the more recent attacks focused on producing the maximum destruction, casualties and impact.

THE CYBER DIMENSION

Today, tremendous destructive potential fits into easily transported packages (bombs, nerve gas and biological agents), and the computers that are connected to the Internet can be attacked from any point on the globe. The threat of retaliation, effective against nations, is less so against small and elusive groups who strike anonymously and have no territory to hold at risk.

The need for the heightened security of critical operations has grown markedly in recent years as a result of the escalation in the use of information technology to improve performance, increased competitive pressures from deregulation and globalization, and the concentration of operations in a smaller number of facilities to decrease costs, with the resulting reduction in redundancy and reserve capacity.

The Computer Security Institute (CSI), which conducts an annual Computer Crime and Security Survey with the participation of the Federal Bureau of Investigation's (FBI) Computer Intrusion Squad in San Francisco, has reported in its 2001 survey that the losses of 186 respondents totaled approximately $378 million. These losses are based on serious computer security breaches detected primarily by large corporations, government agencies, and universities.

Security breaches detected by respondents include a diverse array of attacks such as: unauthorized access by insiders, denial of service attacks, system penetration by outsiders, theft of proprietary information, financial fraud, and sabotage of data and networks. Supervisory

Control And Data Acquisition (SCADA) systems are particularly vulnerable when they use the Internet to monitor and control processes at remote sites. Such a practice is employed in a wide variety of industries including chemical, petrochemical, oil and gas, food processing, pulp and paper, pharmaceuticals, water and wastewater, transportation, energy management, and other manufacturing applications.

Financial losses of course will not be restricted to the theft of proprietary information, financial fraud and other criminal offenses. As more commerce is conducted on-line, civil law suits will increase in which claimants seek downstream damages for network intrusions based on legal theories such as a lack of the "due diligence" owed to stockholders, customers, suppliers, and other innocent third party victims.

China and Russia have publicly acknowledged the role cyber attacks will play in the "next wave of military operations." Two Chinese military officers have published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. Thus, information warfare has arrived as a new concept in military operations. The challenge now is to prevent this weapon from being turned against the United States.

PCCIP

In response to these growing critical infrastructure vulnerabilities, President Clinton in 1996 established the President's Commission on Critical Infrastructure Protection (PCCIP) to study the critical infrastructures that constitute the life support systems of the United States, determine vulnerabilities and propose a strategy for protecting them. The commission in its 1997 report, Critical Foundations: Protecting America's Infrastructures, pointed out that critical infrastructure assurance is a shared responsibility of the public and private sectors.

PDD 63

The report, implemented in 1998 by Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection, declares that federal facilities should be among the first to adopt best practices, active risk management, and improved security planning, thereby presenting a model for industry to follow voluntarily. The PDD calls for the creation of a strong partnership with the business community and state and local governments to maximize the alliance for national security.

The directive also provided for the establishment of the National Infrastructure Protection Center (NIPC) in 1998 by the conversion of the Computer Investigation and Infrastructure Threat Assessment Center into the nucleus of NIPC. NIPC (http://www.nipc.gov) fuses representatives from the FBI, the Departments of Commerce, Defense, Energy, Transportation, the Intelligence Community, and other federal agencies, and the private sector into an unprecedented information sharing effort.

NIPC's mission is to detect, warn of, respond to, and investigate computer intrusions that threaten critical infrastructures. It not only provides a reactive response to an attack that has already occurred, but proactively seeks to discover planned attacks and issues warnings before they occur. This task requires the collection and analysis of information gathered from all available sources (including law enforcement and intelligence sources, data voluntarily provided, and open sources) and dissemination of analysis and warnings of possible attacks to potential victims, whether in the government or the private sector.

The National Infrastructure Protection and Computer Intrusion Program (NIPCIP) consists of FBI agents who are responsible for investigating computer intrusions, implementing the key asset initiative, and maintaining liaison with the private sector. There are about 1,300 pending investigations in the field, ranging from criminal activity to national security intrusions. Many of these cases have a foreign component to them requiring close coordination with FBI legal attaches around the world.

ISACS

PDD 63 also launched a major vehicle for information sharing by encouraging the owners and operators of the critical infrastructures to establish private sector Information Sharing and Analysis Centers (ISACs) to gather, analyze, sanitize and disseminate private sector

information to both industry and the NIPC. The decision to establish an information sharing center is determined by the private sector participants.

ISACs have been established for the critical infrastructure sectors of banking and finance, information and communications, energy, emergency law enforcement and fire services, railroads, and water supply. NIPC promotes the sharing of information with these ISACs and encourages the establishment of ISACs by the remaining sectors.

INFRAGARD

The InfraGard Program is a NIPC effort to build a community of professionals who have a strong interest in protecting their information systems. Members have the opportunity to share information with other members, utilize the law enforcement expertise of the FBI and other law enforcement agencies that participate in the program, and draw on the analytical capabilities of the NIPC. The InfraGard includes representatives from private industry, academic institutions, and other federal, state and local government agencies. It is the most extensive government-private sector partnership for infrastructure protection in the world. A key element of the InfraGard initiative is the confidentiality of reporting by members. Much of the information provided by the private sector is proprietary and is treated as such.

The NIPC plans to promote the expansion of the InfraGard program to other countries, such as Australia, Canada, New Zealand and the United Kingdom.

WARNING PRODUCTS

The NIPC sends out advisories on an ad hoc basis, which are infrastructure warnings to address cyber or infrastructure events with possible significant impact. These are distributed to partners in private and public sectors. The NIPC works in close cooperation with the Federal Computer Incident Response Capability (FedCIRC) to assist federal civil agencies with handling of computer incident responses, and to provide both proactive and reactive security services.

KEY ASSET INITIATIVE

The NIPC role is further strengthened by its Key Asset Initiative (KAI), which maintains a database of information concerning key assets within each FBI field office's jurisdiction, establish lines of communication with key asset owners and operators to share information and work with them to improve their cyber and physical security, and enhance ongoing coordination in the protection of critical infrastructure with other federal, state and local government entities. Listing key assets in the database continually increases, and as of November 1, 8,806 key assets were identified.

TRAINING

Over the past three years, NIPC has provided training for over 4,000 federal, state, local and foreign government investigators through nine core training courses that deal with basic cyber investigations, understanding operating systems, aspects of UNIX, and Cisco Routers. These courses are conducted both at the FBI Academy at Quantico, Virginia and around the United States. The NIPC's training program complements training offered by the FBI's Training Division as well as training offered by the Department of Defense and the National Cybercrime Training Partnership.

INTERNATIONAL OUTREACH

The FBI has established a growing international presence in order to enhance capabilities to counter a broad range of threats, including international terrorism. The FBI currently maintains Legal Attaché (LEGAT) offices in over 40 countries. Forward deployment of FBI personnel has proven a very effective means to establish liaison with counterpart security and intelligence services and to coordinate FBI investigative resources when U.S. interests are attacked or threatened.

The NIPC also maintains an active dialogue with the international community, to include its participation in the Trilateral Seminar of the International Cooperation for Information Assurance in Sweden and the Group of Eight (G-8) Lyon Group (High Tech Crime Subgroup). NIPC personnel have met with government authorities,

both in the US and abroad, from Australia, Canada, Denmark, France, Germany, Israel, Japan, Norway, Singapore, Sweden, the United Kingdom, and other nations over the past year, to discuss infrastructure protection issues with their counterparts. Finally, the NIPC Watch Center is connected to the watch centers of several allies.

The NIPC staff includes government officials on detail from Australia, Canada and the United Kingdom, and it welcomes requests from other U.S. allies for representation on its staff for broadening international cooperation. The NIPC role was further enhanced by the issuance of recent executive orders on cyber protection and homeland security.

CIP INFORMATION AGE EXECUTIVE ORDER

Following the September 11th attacks, President Bush on October 16 issued Executive Order 13231 on Critical Infrastructure Protection in the Information Age, which established the President's Critical Infrastructure Protection Board to coordinate the protection of information systems that involve federal critical infrastructures, and to cooperate with the private sector and state and local governments in the protection information systems that involve their critical infrastructures.

The order also established a panel of approximately 30 corporate chief executive officers to advise the president on the security of information systems supporting the private sector and state and local governments.

CONCLUSION

The threat of cyberterrorism will grow in the New Millennium, as the leadership positions in extremist organizations are increasingly filled with younger, "Internet-savvy" individuals. Most worrisome is a potential coordinated attack on national critical infrastructures. While the United States has not yet experienced this sort of attack, it is not hard to anticipate such a threat from the intrusions we have seen. Cyber attacks know no national boundaries and are truly international in scope and effect. International cooperation and information sharing is critical in order to more effectively respond to this growing threat.

MANY COUNTRIES BENEFIT FROM U.S. ANTITERRORISM TRAINING

By Alan O. Bigler
Director, Antiterrorism Assistance Program,
Diplomatic Security Service, U.S. Department of State

The State Department's Antiterrorism Assistance Program (ATA) has trained over 25,000 foreign police and security forces from 117 different countries in measures designed to combat, deter, and solve terrorist crimes in their countries. ATA Director Alan O. Bigler says that "in the process the program is improving both bilateral and international cooperation in the fight against terrorism."

The U.S. Antiterrorism Assistance Program (ATA) is actively training foreign police and security forces throughout the world to combat, deter, and solve terrorist crimes in their countries. In the process the program is improving both bilateral and international cooperation in the fight against terrorism.

Since its inception, ATA has trained over 25,000 students from 117 different countries, which has had a sizable impact in the fight against international terrorism. In the year 2000 alone, ATA trained 2,741 students from 42 countries (conducting 117 courses in 20 different subject categories), initiated programs in five new countries, participated in 11 technical consultations and conferences, conducted five program evaluations, and performed 20 needs assessments. In the coming years, especially in light of the recent horrific terrorist attacks in New York and Washington, ATA will undergo a major program expansion and is planning accordingly.

During the early 1980s following several serious terrorist incidents throughout the world, it became evident that in countries where such incidents had occurred, many local police and security forces lacked the necessary expertise and equipment to deter and respond in an effective manner. Therefore in 1983, the U.S. Congress authorized the establishment of a special program designed to enhance the antiterrorism skills of friendly countries by providing training and equipment necessary to deter and counter terrorist threats. Congress established the Antiterrorism Assistance Program under an amendment to the Foreign Assistance Act of 1961, which provides its legislative mandate and assigns responsibility for its administration to the State Department's Bureau of Diplomatic Security (DS).

DS Agents, who are sworn federal law enforcement officers, serve as the Regional Security Officer (RSO) at U.S. embassies and other diplomatic missions throughout the world. In this capacity, they are responsible for the security of U.S. facilities and personnel inside the embassy compound, and for ensuring the safety of personnel beyond its walls, including all U.S. citizens that may travel to or visit that country. In order to manage these responsibilities, an RSO must establish and maintain close contacts and working relationships with the host country's security officials, who are tasked with providing external protection and support to the U.S. embassy and staff under long-established diplomatic protocols. Where gaps in a country's capability are noted, the ATA can offer expert assistance.

NEEDS ASSESSMENT IS FIRST STEP

At the embassy's request, and with the concurrence of the Department of State and with the consent of the host country, ATA will send a team of subject matter experts (SMEs) to conduct an extensive and thorough needs assessment of the country's security and police forces. Drawing experts from federal, state and even local law enforcement agencies, ATA sends teams to

provide a critical look at the host nation's key security and law enforcement units. In conducting a needs assessment visit, the experts will frequently meet with senior government and police officials, visit various units, talk to members of the police, and witness capabilities demonstrations in order to determine the type of training and equipment the country will need to meet its particular terrorist threat.

The assessment team considers five basic areas, which are seen as fundamental in any nation's defense against terrorism. Collectively they establish the framework for determining a country's ability to deter and respond to terrorist threats. In general terms, this framework involves the government's ability to:

- Enforce the law, preserve the peace, and protect life and property;
- Protect its national leadership, the seat and functions of government, and its resident diplomatic corps, including that of the United States;
- Control its international borders;
- Protect its critical infrastructure; and
- Manage crises that have national implications.

Upon return, the SMEs compile a report that is presented to ATA's Training Board for review. In addition, a comprehensive country plan is developed that outlines a specific program of training courses and equipment for that country.

Specific assistance is designed to meet identified needs in a variety of police and internal security disciplines. This assistance program is intended to improve functional police skills, mid-level supervision, senior-level management and leadership.

TRAINING IN FUNCTIONAL CATEGORIES

Essentially, ATA training is divided into four separate functional categories: Crisis Prevention, Crisis Management, Crisis Resolution, and Investigations. Each of these four categories contains a number of courses. For example, training in the category of Investigations is provided through a number of specialized courses, two of which are Post-Blast Investigations and Terrorist Crime Scene Investigations, while training in the category of Crisis Resolution could be in the form of a course in Hostage Negotiations.

The bulk of antiterrorism training is provided in the form of highly specialized courses conducted in the United States at one of ATA's several training locations. Course lengths vary from two to five weeks, depending on the subject. Typically, class sizes are held to no more than 24 students. Professional instructors teach courses with simultaneous interpretation into the country's native language by highly experienced interpreters. In addition, course materials are translated into the native language and alphabet, providing students with reference materials they can retain for future use after their return.

In addition to the standard package of courses available, ATA also provides specialized training, consultations, and advisory assistance to address significant security threats. Based on specific, compelling needs, this assistance is often in the form of police administration, management and planning, police instructor training, judicial security, and modern interview and investigative techniques.

ATA also provides limited amounts of specialized equipment. The majority of this equipment is incidental to the courses provided. For example, students who attend the bomb disposal course are given render-safe tools during their training, which they return home with. In addition, where there is a compelling need, and when funds are available, ATA is authorized to provide specialized equipment to meet pressing needs. Although it is presently limited in scope, ATA hopes to expand its equipment grant program in the future to meet the specific needs of its participant nations.

HUMAN RIGHTS

A country's human rights record is a critical element for ATA participation. In full compliance with the Leahy Act, the State Department's Bureau of Democracy, Human Rights, and Labor participates in determining a country's eligibility for participation. Assistance may be suspended if the country's record of human rights practices falls below acceptable standards. U.S. embassies scrupulously screen proposed training

candidates to ensure that no abusers of human rights or officials involved in corrupt practices are permitted to attend training. In addition, ATA instruction incorporates and stresses human rights values and practices in its courses through teaching modern and humane treatment of suspects and members of the general public encountered during police operations.

NEW INITIATIVES

Anti-Kidnapping

In response to a widespread problem of kidnapping for ransom in Colombia and several other Latin American countries, ATA is developing a comprehensive anti-kidnapping training program. The new training program will begin with a kidnapping incident management course that brings together expert instructors with extensive experience in the field to teach a country's security forces, police and government agencies how to manage an incident of kidnapping for ransom. ATA anticipates there will be a great deal of interest in this type of training.

Pipeline Security

In response to concerns expressed by several Central Asian countries, ATA is developing a course that will teach energy pipeline security. Given the vast petroleum resources in the region, and the need for an extensive pipeline network for export, the governments of this region are increasingly concerned with their security. ATA hopes to have a pilot course available within the near future to help address their concerns.

Countering Weapons of Mass Destruction (WMD)

A major new area of training for ATA addresses the problems of managing the effects of a terrorist attack using chemical, biological, or radioactive materials, which are referred to as WMD. Such attacks present significant problems that are new, different, and of much greater scope than terrorist incidents involving conventional weapons.

Courses have been developed and implemented to train foreign "first responders" — police officers, firefighters, paramedics, and emergency room staff — to cope with the complications of responding to terrorist attacks using chemical, biological, or radioactive weapons. These types of attacks can be more deadly than the 1998 massive truck bombs that destroyed the U.S. embassies in East Africa and the recent attacks on the World Trade Center in New York and the Pentagon. The ATA "first responder" program mirrors the U.S. Government's domestic program. As much as possible, the training and equipment will be the same as that provided to first responders in the United States.

Terrorist Financing

The ATA program, working with experts in other agencies, is developing programs to help foreign officials to counter terrorist fund raising. In recent years, international terrorist organizations have relied less and less on state sponsors for their financing and other material support. However, many of these groups have founded charities and service organizations as fronts through which they seek contributions from people who believe they are for legitimate purposes. Some terrorist groups also operate legitimate businesses as front companies to raise money or facilitate transfers. A course designed to teach investigators how to trace, follow and link terrorist groups with their funds has been developed and was presented to a test country in July 2001. This pilot course was very well received and should become available for general offering.

ATA Results and Impact

ATA training provides the participant country police and security forces with a cadre of trained officers familiar with American values and thinking, on whom the RSO and other U.S. officials can rely in times of crisis. ATA training has also been widely credited with increasing the confidence, and in turn, the professionalism of students who have completed the training. In many countries, follow-up program reviews have determined that these officers have not only grown in skill and confidence, but also have advanced beyond their peers in promotion and stature due to the knowledge and training gained from their ATA training.

In addition to providing individual students with enhanced training, there are numerous examples where

ATA training has directly thwarted or solved several major terrorist incidents or major crimes. For example, in one country, ATA-trained police, using the techniques they learned during Surveillance Detection training, arrested two terrorists with a bomb in their possession outside the home of a judge. In another, an ATA-trained Police Crisis Response Team was deployed to the presidential palace of a country during an attempted coup d'etat, thus thwarting an overthrow of the government. In still another, a graduate of the ATA course in Police Crisis Management was called upon to respond to a crisis situation at a nightclub that was firebombed with 13 people killed and numerous others injured. This officer attributes his ATA training in crisis management as key to his ability to handle the subsequent panic and confusion of the situation.

Connecting with ATA

To learn more about ATA, the program office operates its own Internet Web site, which can be found at http://www.diplomaticsecurity.org.

TERRORISM AND COUNTERTERRORISM AFTER SEPTEMBER 11TH

By Bruce Hoffman
Vice President, External Affairs Director, RAND Corporation Washington Office

The enormity and sheer scale of the simultaneous suicide terrorist attacks on September 11 eclipses anything previously seen — either individually or in aggregate, says Bruce Hoffman, vice president and director of the RAND Washington office. "It calls, unquestionably, for a proportionate response of unparalleled determination and focus such as we see today in our actions both in the United States and abroad, as well as one that utilizes the full range of formidable tools at our disposal — diplomatic, military, and economic."

THE 9/11 ATTACKS IN CONTEXT

Until September 11th, a total of no more than perhaps 1,000 Americans had been killed by terrorists either in this country or abroad since 1968 — the year credited with marking the advent of the modern era of international terrorism when the Popular Front for the Liberation of Palestine (PFLP) hijacked an El Al flight on July 23. To put the events of that tragic day further in context, until the attacks on the World Trade Center and Pentagon, no terrorist operation had killed more than 500 persons at one time.[1] Whatever the metric, the enormity and sheer scale of the simultaneous suicide attacks of that day eclipse anything we have previously seen — either individually or in aggregate. Accordingly, for that reason alone, September 11th argues for nothing less than a re-configuration of both our thinking about terrorism and how we both prepare and organize to counter it. Such a change is amply justified by the unique constellation of operational capabilities evident in that day's tragic attacks: showing a level of planning, professionalism and tradecraft rarely seen among the vast majority of terrorists and terrorist movements we have known.[2] Among the most significant characteristics of the operation were its:

- ambitious scope and dimensions;
- consummate coordination and synchronization;
- professionalism and tradecraft that kept so large an operation so secret; and
- the unswerving dedication and determination of the 19 aircraft hijackers who willingly and wantonly killed themselves, the passengers and crews of the four aircraft they commandeered and the thousands of persons working in or visiting both the World Trade Center and the Pentagon.

The significance of the September 11th incidents from a terrorist operational perspective is that simultaneous attacks — using far more prosaic and arguably conventional means of attack (such as car bombs, for example) — are relatively uncommon. For reasons not well understood, terrorists typically have not undertaken such coordinated operations. This was doubtless less of a choice than a reflection of the logistical and other organizational hurdles that most terrorist groups are not able to overcome. Indeed, this was one reason why we were so galvanized by the synchronized attacks on the American embassies in Nairobi and Dar es Salaam three years ago. The orchestration of that operation, coupled with its unusually high death and casualty tolls, stood out in a way that, until September 11th, few other terrorist actions had: bringing bin Laden as much renown as infamy in many quarters.

---

1. Approximately 440 persons perished in a 1979 fire deliberately set by terrorists at a movie theater in Abadan, Iran.

2. Nor is this a particularly "American-centric" view in reaction to the stunning and tragic events of two months ago. For example, an old friend and colleague, who is one of Israel's leading counterterrorist experts, and who has long experience in military, the government and academe was totally shocked by the September 11th attacks — specifically, their coordination, daring and lethality — remarking: "Never could I have imagined that terrorists could or would do that" (telephone conversation, 17 September 2001). I am also reminded of a conversation with a senior, highly decorated Sri Lankan Armed Forces brigade commander and military intelligence operative who once explained in great detail the "difficulties of pulling off even a successful, significant terrorist attack" (discussion, Batticola, Sri Lanka, December 1997)-not least the four orchestrated suicide aircraft hijackings and crashes that occurred on September 11th.

During the 1990s, perhaps only one other (presumably unrelated) terrorist incident evidenced those same characteristics of coordination and high lethality: the series of attacks that occurred in Bombay in March 1993, where a dozen or so simultaneous car bombings rocked the city, killing nearly 300 persons and wounding more than 700 others.[3] Indeed, apart from the attacks on the same morning in October 1983 of the U.S. Marine barracks in Beirut and a nearby French paratroop headquarters, and the IRA's near-simultaneous assassination of Lord Mounbatten and remote-control mine attack on British troops in Warrenpoint, Northern Ireland, in 1979, it is hard to recall many other significant incidents reflecting such operational expertise, coordination and synchronization.

WHERE WE WENT WRONG IN FAILING TO PREDICT THE 9/11 ATTACKS

Accordingly, we were perhaps lulled into believing that mass, simultaneous attacks in general, and those of such devastating potential as we saw in New York and Washington on September 11th, were likely beyond most capabilities of most terrorists — including those directly connected to or associated with Osama bin Laden. The tragic events of that September day demonstrate how profoundly misplaced such assumptions were. In this respect, we perhaps overestimated the significance of our past successes (e.g., in largely foiling most of bin Laden's terrorist operations during the period between the August 1998 embassy bombings and the November 2000 attack on the USS Cole) and the terrorists' own incompetence and propensity for mistakes (e.g., Ahmad Ressam's bungled attempt to enter the United States from Canada in December 1999). Indeed, both more impressive and disturbing is the fact that there was likely considerable overlap in the planning for these attacks and the one last November against the USS Cole in Aden: thus suggesting a multi-track operational and organizational capability to coordinate major, multiple attacks at one time.

Attention was also arguably focused too exclusively either on the low-end threat posed by car and truck bombs against buildings or the more exotic high-end threats, involving biological or chemical weapons or cyber-attacks. The implicit assumptions of much of our planning scenarios on mass casualty attacks were that they would involve germ or chemical agents or result from widespread electronic attacks on critical infrastructure and that any conventional or less extensive incident could be addressed simply by planning for the most catastrophic threat. This left a painfully vulnerable gap in our anti-terrorism defenses where a traditional and long-proven tactic — like airline hijacking — was neglected in favor of other, less conventional threats, and the consequences of using an aircraft as a suicide weapon seem to have been almost completely discounted.

In retrospect, it arguably was not the 1995 sarin nerve gas attack on the Tokyo subway and nine attempts to use bio-weapons by Aum that should have been the dominant influence on our counterterrorist thinking, but a 1986 hijacking of a Pan Am flight in Karachi, where the terrorists' intentions were reported to have been to crash it into the center of Tel Aviv, and the 1994 hijacking in Algiers of an Air France passenger plane by terrorists belonging to the Armed Islamic Group (GIA), who similarly planned to crash the fuel-laden aircraft with its passengers into the heart of Paris. The lesson, accordingly, is not that we need to be unrealistically omniscient, but rather that we need to be able to respond across a broad technological spectrum of potential adversarial attacks.

We also had long consoled ourselves — and had only recently begun to question and debate the notion — that terrorists were more interested in publicity than killing and therefore had neither the need nor interest in annihilating large numbers of people. For decades, there was widespread acceptance of the observation made famous by Brian Jenkins in 1975 that, "Terrorists want a lot of people watching and a lot of people listening and not a lot of people dead."[4] Even despite the events of the mid-1980s — when a series of high-profile and particularly lethal suicide car and truck-bombings were directed against American diplomatic and military targets in the Middle East (in one instance resulting in the deaths of 241 Marines) — many analysts saw no need to revise these arguments. In 1985, Jenkins, one of the most perspicacious and acute observers of this phenomenon, again noted that,

3. Celia W. Dugger, "Victims of '93 Bombay Terror Wary of U.S. Motives," New York Times, 24 September 2001

4. Brian Michael Jenkins, "International Terrorism: A New Mode of Conflict" in David Carlton and Carlo Schaerf (eds.), International Terrorism and World Security (London: Croom Helm, 1975), p. 15.

"simply killing a lot of people has seldom been one terrorist objective . . . Terrorists operate on the principle of the minimum force necessary. They find it unnecessary to kill many, as long as killing a few suffices for their purposes."[5] The events of September 11th prove such notions now to be wishful thinking, if not dangerously anachronistic. On that day, bin Laden arguably wiped the slate clean of the conventional wisdom on terrorists and terrorism and, by doing so, ushered in a new era of conflict, more bloody and destructive than before.

Finally, bin Laden himself has re-written the history of both terrorism and probably of the post-Cold War era — which he arguably single-handedly ended on September 11th. At a time when the forces of globalization, coupled with economic determinism, seemed to have submerged the role of the individual charismatic leader of men beneath far more powerful, impersonal forces, bin Laden has cleverly cast himself (admittedly and inadvertently with our assistance) as a David against the American Goliath: one man standing up to the world's sole remaining superpower and able to challenge its might and directly threaten its citizens. To his followers, bin Laden has proven to be the fabled right man in the right place at the right time: possessing the vision, financial resources, organizational skills, and flair for self-promotion to meld together the disparate strands of Islamic fervor, Muslim piety, and general enmity toward the West into a formidable global force.

WHAT NEEDS TO BE DONE

The concept of proportionality has long governed American counterterrorist policy. Its American proponents argued, and our many allies throughout the world expected, that the American military response would be commensurate with the terrorist attack that provoked it. Thus, in 1986, when the Qadhafi regime was implicated in the bombing of a West Berlin discotheque frequented by American soldiers, the United States retaliated with airstrikes directed against Libyan military targets in Tripoli and Benghazi — including Muammar Qadhafi's living quarters — in an attempt to eliminate the Libyan leader himself. Similarly, in 1998, when bin Laden was identified as the architect of the massive truck bombings of the American embassies in Kenya and Tanzania, the U.S. launched nearly 100 cruise missiles against his training camps in Afghanistan — also in hopes of killing him — as well as against a pharmaceutical factory allegedly linked to bin Laden and believed to be manufacturing chemical weapons in the Sudan. Two Americans had lost their lives in the discotheque bombing and twelve in Nairobi. In the latter case, the response may have been insufficient. But our situation today leaves no room for quibbling.

As previously noted, the enormity and sheer scale of the simultaneous suicide attacks on September 11 eclipses anything we have previously seen — either individually or in aggregate. It calls, unquestionably, for a proportionate response of unparalleled determination and focus such as we see today in our actions both in the United States and abroad, as well as one that utilizes the full range of formidable tools at our disposal — diplomatic, military, and economic. While much attention is currently focused on the military options being exercised in South Asia, they are only one instrument that the United States can bring to bear in the struggle against terrorism. Our efforts need to be fully coordinated, sustained, and prolonged. They will require commitment, political will, and patience. They must have realistic goals and not unduly raise or create false expectations. And, finally, they must avoid cosmetic or "feel-good" physical security measures that contribute only tangentially, if at all, to the enhancement of national as well as international security.

In conclusion, it must be appreciated that the struggle against terrorism is never-ending. By the same token, our search for solutions and new approaches must be equally continuous and unyielding, proportional to the threat posed by our adversaries in both innovation and determination.

5. Brian Michael Jenkins, The Likelihood of Nuclear Terrorism (Santa Monica, CA: The RAND Corporation, P-7119, July 1985), p. 6.

The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. Government.

ANTHRAX AND MASS-CASUALTY TERRORISM: WHAT IS THE BIOTERRORIST THREAT AFTER SEPTEMBER 11?

By Jason Pate
Senior Research Associate and Manager, Weapons of Mass Destruction Terrorism Project
Monterey Institute of International Studies

"Trends in terrorism over the past 15 years indicate that loosely linked transnational networks motivated primarily by religious ideologies seeking mass casualties are replacing more 'traditional' terrorists who are motivated primarily by politics," says Jason Pate, a senior research associate at the Monterey Institute of International Studies. "These ominous trends suggest the potential for mass-casualty attacks, and because biological agents could be used in this fashion, the potential for mass-casualty bioterrorism may be at hand."

INTRODUCTION

The unprecedented terrorist attacks on September 11 and the subsequent series of anthrax attacks have ushered in a new era of terrorism in the United States. Although there previously have been relatively large-scale terrorist attacks in America, such as the 1995 Oklahoma City bombing, the coordination, planning, and scale of the September 11 attacks demonstrate that mass-casualty terrorism has reached the U.S. homeland.

Even bioterrorism is not a new phenomenon in U.S. history. In 1984 a cult in a small Oregon town used salmonella to contaminate salad bars in an effort to influence a local election. The cult, which chose an incapacitating rather than lethal agent, succeeded in making 751 people ill, but no one died. In 1994 and 1995, four men, all members of an extremist antigovernment group in Minnesota called the Patriots Council, were the first people ever convicted of possession of a biological agent for use as a weapon under the 1989 Biological Weapons Antiterrorism Act. The men acquired the protein toxin ricin, which is derived from castor beans, possibly to use against local law enforcement and federal officials. Although the Patriots Council plan was never carried out, the group was heavily influenced by rightwing extremist Christian Identity ideology, similar to the ideology that influenced Timothy McVeigh.

Even though both bioterrorism and large-scale conventional terrorism were threats to the United States prior to September 11, the events of the last two months have shown that a quantum leap in terrorist tactics may be occurring. Trends in terrorism over the past 15 years indicate that loosely linked transnational networks motivated primarily by religious ideologies seeking mass casualties are replacing more "traditional" terrorists who are motivated primarily by politics — such as creating a homeland or seeking justice for perceived oppression by the target state. These ominous trends suggest the potential for mass-casualty attacks, and because biological agents could be used in this fashion, the potential for mass-casualty bioterrorism may be at hand.

This article reviews the historical context of the current anthrax attacks, paying special attention to looking at the current situation in broad perspective. Then it explores why the United States is so vulnerable to this type of terrorism and offers policy recommendations to address these vulnerabilities.

THE CURRENT ANTHRAX ATTACKS

In spite of hundreds of anthrax hoaxes since 1998, the recent anthrax attacks are an unprecedented event. Never before in U.S. history has a biological warfare agent been used in war or peacetime against Americans.

It is no surprise that anthrax is the agent of choice, from both technical and political perspectives. On the technical side, anthrax is the prototypical biological weapons agent — it is relatively easy to produce, it is extremely virulent, and the infection is not contagious, so the outbreak will not spread beyond those affected directly. Most importantly, anthrax forms rugged spores when exposed to environmental stresses, and these spores facilitate processing and weaponization.

From a political perspective, since 1995 there has been very high-level political and media attention given to anthrax. In the mid-to-late 1990s, there were great revelations that Iraq, the Soviet Union and later Russia, and South Africa had created extensive biological weapons programs including work on anthrax. In addition, the U.S. military anthrax vaccine program generated extensive controversy over safety allegations that have not been proven in any clinical trials. Finally, the well publicized arrest of a rightwing extremist in 1998 for suspected anthrax possession — he possessed only the harmless anthrax vaccine strain — opened the floodgates for hundreds of anthrax hoaxes nationwide 1998-2001. During the entire period 1995-2001, hundreds of media, academic, and government reports highlighted the vulnerability of the United States to biological terrorism, perhaps emphasizing to potential terrorists not only that the United States was not prepared to deal with bioterrorism, but also that the American public was terrified of the possibility.

A number of issues are critical to understanding the bioterrorist threat beyond September 11, including determining who used the anthrax and why they used it. The quality of the anthrax used in the recent attacks has been a matter of discussion. Clearly, the anthrax was processed using relatively sophisticated techniques, and there are some indications that chemical additives were added to help make the spores more effective. These technical details seem to point to the involvement of a state in the attacks. However, more questions than answers remain. Without knowing who perpetrated the attacks, it is very difficult to prepare for the future. Do the perpetrators have a limited supply of anthrax, or do they have an ongoing production capability?

Perhaps even more important is the motivation of the attackers. Thus far, the attacks have not been designed to affect large numbers of people and have been accompanied by warning letters identifying both that an attack had occurred and what agent was involved. In addition, the letters do not represent an effective delivery system — very few people have been affected. Future larger-scale attacks may not come with such clear indicators. In order to maximize casualties, anthrax attackers would not announce that an incident had occurred. Rather, people would begin exhibiting symptoms and would die, and it would be up to the public health system to identify that an attack had occurred, by which time it would probably be too late to save many victims.

In sum, the recent anthrax attacks occurred in a historical context. Although the attacks are unprecedented, they should not necessarily come as a surprise. Fortunately, the attacks have been very limited, but the potential exists for a much larger-scale aerosol delivery resulting in mass casualties.

WHY THE UNITED STATES IS VULNERABLE TO MASS-CASUALTY BIOTERRORISM

The United States is a vast, open society that by its very nature is vulnerable to terrorism in general. U.S. borders are open to both goods and people, interstate movements are virtually unregulated, and there has never before been a good reason to implement changes. Of the range of terrorist threats — from truck bomb to plane hijacking to anthrax attack to smallpox epidemic — that could cause mass casualties, the United States is perhaps least able to deal with bioterrorism. Whereas security measures can be implemented at airports to eliminate the possibility of a repeat of September 11, and potential target structures can be made less vulnerable to conventional attack, there is no quick and straightforward solution to the bioterrorism problem.

One of the reasons the United States is so vulnerable to bioterrorism is because successive federal, state, and local governments in the country have allowed the U.S. public health infrastructure to deteriorate over the last three decades. After successful pathogen eradication campaigns, the advent of powerful antibiotics, and the

emergence of a largely healthy middle and upper class, public health in the 1970s did not seem a high priority in an era of budget cuts. Today, the public health system across the United States barely has enough funding, staff, and other resources to manage day-to-day issues, much less crises caused by either natural outbreaks or bioterrorism. The United States simply does not have the capacity to manage a disease outbreak affecting hundreds or thousands of people.

At the international level, there are very few tools that are effective against the bioterrorist threat. The 1972 Biological and Toxin Weapons Convention (BWC) is the main international treaty governing biological weapons. Other mechanisms exist, such as the Australia Group, which attempts to provide guidelines for technology exports related to biological weapons production. But the Australia Group has limited enforcement power and does not include certain key states of concern. In addition, the Group limits only relatively large-capacity equipment; this does not address the possibility of smaller-scale clandestine production. The BWC itself has no enforcement of verification regime, and although a draft Protocol was submitted to the BWC's Conference of States Parties this year, the United States refused to sign the document, effectively halting work on augmenting the treaty's ability to enforce its provisions. A BWC Review Conference is scheduled for November 2001, although it is unclear whether there will be any more progress toward a verification agreement.

However, even with U.S. signature and a completed Protocol, it is far from clear that the BWC would do anything in the fight against bioterrorism other than help to build and strengthen the international norm against biological weapons. Indeed, the treaty text does not address terrorism but focuses instead on the threat from states.

At the national policy level, the concepts of deterrence and foreign policy that were so useful during the Cold War do not apply to the threat of bioterrorism. When the adversary is an elusive network of enigmatic diehard operatives completely dedicated to their cause, it is nearly impossible to design a strategy to respond. Terrorists rarely have targetable assets, either financially or militarily. Efforts to freeze terrorist financial assets are hampered by the vastness of the international banking system, and only in cases where states are supporting terrorists is it possible to find a military target. All attempts to destroy al-Qaida's infrastructure are laudable, and the United States should continue to pursue the perpetrators of the September 11 attacks. But it is crucial to remember that these efforts have limited value.

In sum, the vulnerability of the United States to bioterrorism, the lack of effective international means, and ingrained Cold War foreign policy concepts make responding to the bioterrorist threat exceedingly complex and challenging.

POLICY RECOMMENDATIONS

Policies to address the bioterrorist threat come in three broad categories: addressing terrorism generally, responding to a mass-casualty bioterrorist incident specifically, and maximizing all available international options.

The United States should continue to use all means at its disposal to eliminate the current terrorist threat from al-Qaida and related organizations. This includes raising the costs of sponsoring terrorism so high that terrorists will not be able to operate easily; maximizing intelligence operations directed against terrorism; and making it clear that terrorism is unacceptable, in order to deter future attacks. In addition, the United States should work very closely with its international partners to coordinate efforts designed to reduce the biological weapons threat. Security will be increased if the taboos against biological weapons are strengthened and the international community works together to address the threat.

There are limits to what the United States can do nationally and internationally to address bioterrorism. Therefore, policymakers should accept that it is impossible to eliminate completely either the terrorist threat or the threat from bioterrorism. It is therefore highly critical that the United States prepare itself to detect and respond to a bioterrorist incident. This includes steps to:

- Immediately augment the public health system. This includes increasing funding and resources that will enable the public health system to increase its capacity.

- Design and implement an extensive surveillance network for disease outbreaks.

- Link all health providers to the Internet, and create online resources that will serve as the central repository for disease information. Real-time data will enable health officials to monitor public health and identify critical developments before they become unmanageable.

- Upgrade laboratory capabilities so that many more labs have the ability to identify pathogens using standardized procedures which will also need to be developed.

- Educate and inform all health-care providers to recognize the signs and symptoms of suspicious outbreaks.

(The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. Government.)

BRINGING TERRORISTS TO JUSTICE UNDER THE RULE OF LAW

By Peter Raven-Hansen
Glen Earl Weston Research Professor of Law, The George Washington Law School

"Bringing terrorists to justice under the rule of law is a slow, cumbersome, inefficient business," says George Washington Law School Professor Peter Raven-Hansen. Nevertheless, the United States continues to apply the rule of law in the investigation and prosecution of the global war on terrorism. "The United States has responded to terrorist attacks with the same tools of criminal justice: surveillance, arrest, detention, and trial."

The history of lawless police states leaves little doubt how one would respond to a terrorist attack. The government would declare a national emergency to invoke new "emergency" powers and measures. Already secretly tracking many citizens, the police would expand surveillance in a search for the attackers. They would quickly arrest suspects, potential witnesses, and maybe dissidents and critics as well. The arrested would be held in isolation and possibly abused to make them talk. Finally, the authorities would first secretly decide who is guilty (or who should be called guilty) and afterwards announce that judgment in show trials, followed by execution or long terms of imprisonment.

A lawless response would be swift and seemingly efficient because it could be decided personally by one or a few men whose orders are "law" to their underlings.

The United States has responded to terrorist attacks with the same tools of criminal justice: surveillance, arrest, detention, and trial. But in a state ruled by law rather than personal fiat, these tools are not crafted by President Bush and his counselors. They were instead authorized by pre-existing laws in the U.S. Constitution, legislation enacted by Congress, and executive regulations. Furthermore, with few exceptions, the only U.S. "emergency powers" are ones given the President by laws which Congress has previously passed, not ones he gives himself because he thinks it necessary. And if the tools provided by law prove to be too slow and cumbersome to meet the terrorist threat, they must be changed by a public legislative process, not by presidential order.

SURVEILLANCE

The U.S. Constitution protects the people from "unreasonable searches and seizures." To be reasonable, a search — whether conducted physically in the home or electronically by wiretap or other communications intercept — must ordinarily be pre-approved by an independent judge on evidence showing that there is probable cause to believe that evidence of a crime will be found. Evidence obtained in violation of these standards can be thrown out of court. But the U.S. Supreme Court has recognized that collecting security intelligence is different from collecting evidence of a crime, partly because it is needed to prevent spying or terrorism and not just to solve completed crimes. Congress has therefore enacted a law permitting independent judges to authorize surveillance for the purpose of collecting foreign intelligence on a lesser showing of probable cause. The government need only show that there is probable cause to believe that the target of the surveillance is a foreign agent or international terrorist.

Such foreign intelligence surveillance was already being conducted before the September 11 attacks on the United States, and, indeed, had produced crucial evidence against the terrorists who were ultimately tried for the 1998 bombings of the U.S. embassies in Tanzania and Kenya. But the law before September 11 also restricted some surveillance. U.S. newspapers report, for example, that before September 11 the government was unable to make the showing required to obtain surveillance of one of the men now suspected

of participating in the September 11 attacks. In addition, the pre-September 11 foreign surveillance law was technologically obsolete in some respects. It was intended to apply chiefly to traditional telephone wiretaps and was not well-suited to email and other means of communications developed since the law was enacted.

The Bush administration therefore sought changes in the law from Congress after the September 11 attack. Because the U.S. lawmaking process is public, so was the ensuing debate in Congress and in the U.S. mass media. Defenders of privacy resisted many of the changes sought by the Administration, and proponents of greater security promoted them. In the end, some compromises were made in a new law expanding security surveillance. Yet the new law still falls short of the unrestricted surveillance which we would expect in a police state. An independent judge must still approve security surveillance, it must still be directed at foreign agents or international terrorists, with special protections for U.S. citizens in many cases, and it is still not open-ended.

ARREST AND DETENTION

In the first seven weeks of its investigation of the September 11 attacks, the Federal Bureau of Investigation detained over 1,100 persons. But the U.S. Constitution protects a person from unreasonable "seizure" — arrest and detention — as well as from unreasonable search. There is no law which allows general "preventative detention" — detaining a person indefinitely in order to prevent him from committing a crime in the future — except for enemy aliens in war. The police may stop someone for questioning only on reasonable suspicion that he has been or is involved in criminal activity and may detain him only temporarily before charging him with a crime.

The arrest of most of the 1,100 met this standard, but not because they were reasonably suspected of being involved in the September 11 attack. Instead, they were arrested on suspicion of committing what the U.S. Attorney General called "spitting on the sidewalk": minor crimes like traffic violations, using false identities, or credit card fraud. Detention without bail for persons suspected of such minor crimes is unusual; often even conviction for such crimes carries no jail sentence. Consequently, the "spitting-on-the-sidewalk" detentions have been the subject of growing debate in the media, and defenders of civil liberties have insisted that the government is really embarked on an unprecedented and legally controversial policy of preventative detention to meet the threat of terrorism.

Another 200 detainees are aliens who are reasonably suspected of violating their immigration status in the United States, by, for example, overstaying their student visas. Before September 11, however, persons suspected of minor "overstays" were hardly ever detained for more than a short period while they awaited immigration proceedings. The continued detention of such aliens in the September 11 investigation has also been criticized as preventative detention.

Nevertheless, there is an essential difference between the wholesale and unrestricted round-up of suspects and dissidents which we would expect in a lawless police state and the September 11 detentions. It is that the U.S. government has been obliged publicly to justify its arrests by law, even if its justifications have been criticized. In addition, the detainees have rights under U.S. law while they are detained. A detainee has the right to call a lawyer, and if the detainee is charged with a crime, he has a right to have a lawyer appointed for him at government expense. The Department of Justice has asserted that each detainee has been informed of this right, although questions remain about how easy it has been for detainees to exercise the right. Detainees also have a right to be protected from physical abuse during their detention. No one has yet credibly complained that this right has been violated.

Under the rule of law, it is usually preferable to change law when it no longer meets perceived social needs than to bend it, let alone break it. In fact, the Attorney General did ask Congress for new authority to detain a person indefinitely if he had reason to believe that the person was a terrorist or was likely to commit a terrorist act. Despite the terrorist emergency, Congress rejected that request, doubting that such an expansion of detention authority was necessary or constitutional. Instead, it has given him new but limited authority to detain aliens for short periods before starting immigration proceedings against them.

TRIAL

The U.S. Constitution guarantees a bundle of important rights to a person charged with a crime. First, and perhaps most important, he has the right to a speedy and public trial. He has the right to confront the witnesses and see the evidence against him. He has a right to a lawyer at the government's expense. He has the right to ask for a jury of impartial ordinary citizens to decide whether the evidence shows his guilt "beyond a reasonable doubt." And he has the right to see any evidence which the government has found which might show his innocence.

These rights were afforded the terrorists who were tried in U.S. courts for the 1993 World Trade Center bombing, the 1995 Oklahoma City bombing, and the 1998 embassy bombings. In the latter case, for example, lawyers for defendants — indicted along with Osama bin Laden as members of the al-Qaida network — succeeded during a five-month trial in having some criminal charges dismissed, some surveillance declared unlawful, and some evidence against them thrown out of court. Nevertheless, after hearing 205 witnesses, the jury found beyond a reasonable doubt that defendants were guilty of bombing the U.S. embassies.

Despite the government's unbroken record of success in terrorist prosecutions, however, they have not been problem-free. A major drawback in trying terrorists is that some of the evidence against them (or which they are entitled to see) may have been obtained from secret intelligence sources and methods. Disclosure of the evidence may jeopardize such sources and methods. In one terrorism prosecution, for example, the government had to disclose evidence which had been obtained by an electronic intercept of a communication by the al Qaeda network. Within a short time after the disclosure, the network reportedly stopped using that channel of communication and the intelligence source was lost.

The obvious solution to this risk — keeping the evidence secret from the terrorist defendant and his lawyers — is prohibited by U.S. law. In non-criminal immigration proceedings to remove suspected terrorist aliens from the United States, however, the government has tried to use secret evidence when it was necessary to protect intelligence sources and methods. This use of secret evidence, however, may also be unlawful. At least three lower courts have rejected immigration decisions in such cases on the ground that using secret evidence violates the right of aliens to the due process of law guaranteed by the Constitution. But these decisions did not dictate whether the government is permitted to use secret evidence in other parts of the country, and the Supreme Court — which could decide this question for the entire nation — has not yet done so.

Consequently, before September 11, some members of Congress proposed a law which would have prohibited the immigration authorities from using secret evidence. After September 11, the support for such a law has, at least temporarily, evaporated. Courts must therefore continue to decide case by case whether secret evidence can be used in immigration proceedings until the Supreme Court or Congress settles the question.

CONCLUSION

Bringing terrorists to justice under the rule of law is a slow, cumbersome, inefficient business. It may even be an unsuccessful business, if essential evidence is excluded because it was obtained by unlawful surveillance, if the government decides that it cannot risk disclosure of intelligence sources and methods, or if the proof does not show guilt beyond a reasonable doubt (even though it shows that it is more probable than not that defendant is guilty). But as the Supreme Court once said in deciding to free a terrorist who had been unlawfully tried during the Civil War:

> The power of punishment is alone [available] through the means which the laws have provided for that purpose, and if they are ineffectual, there is an immunity from punishment, no matter ... how much ... crimes may have shocked the ... country, or endangered its safety. By the protection of law human rights are secured; withdraw that protection, and they are at the mercy of wicked rulers, or the clamor of an excited people.

In its quest for protection from terrorists, the United States will never give up the protection of law. ◉

(The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. Government.)

INTERNATIONAL TERRORISM: AMERICAN HOSTAGES

The Office of Counterterrorism, headed by Ambassador Francis X. Taylor, coordinates all U.S. Government efforts to improve counterterrorism cooperation with foreign governments. The Coordinator chairs the Interagency Working Group on Counterterrorism and the State Department's terrorism task forces to coordinate responses to major international terrorist incidents that are in progress. The Coordinator has primary responsibility for developing, coordinating, and implementing American counterterrorism policy.

U.S. COUNTERTERRORISM POLICY

- First, make no concessions to terrorists and strike no deals;
- Second, bring terrorists to justice for their crimes;
- Third, isolate and apply pressure on states that sponsor terrorism to force them to change their behavior; and
- Fourth, bolster the counterterrorism capabilities of those countries that work with the U.S. and require assistance.

The United States Government will make no concessions to terrorists holding official or private U.S. citizens hostage. It will not pay ransom, release prisoners, change its policies, or agree to other acts that might encourage additional terrorism. At the same time, the United States will use every appropriate resource to gain the safe return of American citizens who are held hostage by terrorists. Hostage-taking is defined under international law (International Convention Against the Taking of Hostages, adopted December 17, 1979) as the seizing or detaining and threatening to kill, injure, or continue to detain a person in order to compel a third party to do or abstain from doing any act as an explicit or implicit condition for the release of the seized or detained person.

It is internationally accepted that governments are responsible for the safety and welfare of persons within their borders. Aware of both the terrorist threat and public safety shortcomings in many parts of the world, the United States has developed enhanced physical and personal security programs for U.S. personnel and has established cooperative arrangements with the U.S. private sector. It also has established bilateral counter-terrorism assistance programs and close intelligence and law enforcement relationships with many nations to help prevent terrorist incidents or to resolve them in a manner that will deny the perpetrators benefits from their actions.

The United States also seeks effective judicial prosecution and punishment for terrorists and criminals victimizing the United States Government or its citizens and will use all legal methods to these ends, including extradition. U.S. policy and goals are clear, and the United States Government actively pursues them alone and in cooperation with other governments.

The United States Government believes that paying ransom or making other concessions to terrorists in exchange for the release of hostages increases the danger that others will be taken. Its policy therefore rejects all demands for ransom, prisoner exchanges, and deals with terrorists in exchange for the release of hostages. At the same time, it will make every effort, including contact with representatives of the captors, to obtain the release of the hostages.

The United States strongly urges American companies and private citizens not to pay ransom. It believes that good security practices, relatively modest security expenditures, and continual close cooperation with embassy and local authorities can lower the risk to Americans living in high-threat environments.

The United States Government is concerned for the welfare of its citizens but cannot support requests that

host governments violate their own laws or abdicate their normal law enforcement responsibilities. On the other hand, if the employing organization or company works closely with local authorities and follows U.S. policy, U.S. Foreign Service posts can actively pursue efforts to bring the incident to a safe conclusion. This includes providing reasonable administrative services and, if desired by the local authorities and the American organization, full participation in strategy sessions. Requests for United States Government technical assistance or expertise will be considered on a case-by-case basis. The full extent of United States Government participation must await an analysis of each specific set of circumstances.

If a U.S. private organization or company seeks release of hostages by paying ransom or pressuring the host government for political concessions, U.S. Foreign Service posts will limit their participation to basic administrative services, such as facilitating contacts with host government officials. The host government and the U.S. private organization or citizen must understand that if they wish to follow a hostage resolution path different from that of United States Government policy, they do so without its approval or cooperation. The United States Government cannot participate in developing and implementing a ransom strategy. However, U.S. Foreign Service posts may maintain a discreet contact with the parties to keep abreast of developments.

Under current U.S. law 18 USC 1203 (Act for the Prevention and Punishment of the Crime of Hostage-Taking, enacted October 1984 in implementation of the U.N. Convention on Hostage-Taking), seizure of a U.S. national as a hostage anywhere in the world is a crime, as is any hostage-taking action in which the United States Government is a target or the hostage-taker is a U.S. national. Such acts, therefore, are subject to investigation by the Federal Bureau of Investigation and to prosecution by U.S. authorities. Actions by private persons or entities that have the effect of aiding and abetting the hostage-taking, concealing knowledge of it from the authorities, or obstructing its investigation, may themselves be in violation of U.S. law.

Source: Office of the Coordinator for Counterterrorism, U.S. Department of State.

STATE-SPONSORED TERRORISM AND FOREIGN TERRORIST ORGANIZATIONS

The designation of state sponsors of terrorism by the United States — and the imposition of sanctions — is a mechanism for isolating nations that use terrorism as a means of political expression. U.S. policy seeks to pressure and isolate state sponsors so they will renounce the use of terrorism, end support to terrorists, and bring terrorists to justice for past crimes.

Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria continue to be the seven governments that the U.S. Secretary of State has designated as state sponsors of international terrorism.

The following list of terrorist groups is presented in two sections. The first section lists the 28 groups designated by the Secretary of State on October 5, 2001 as Foreign Terrorist Organizations (FTOs), pursuant to section 219 of the Immigration and Nationality Act, as amended by the Antiterrorism and Effective Death Penalty Act of 1996. The designations carry legal consequences:

- It is unlawful to provide funds or other material support to a designated FTO.
- Representatives and certain members of a designated FTO can be denied visas or excluded from the United States.
- U.S. financial institutions must block funds of designated FTOs and their agents and must report the blockage to the U.S. Department of the Treasury.

The second section lists other terrorist groups that were active during 2000. Terrorist groups whose activities were limited in scope in 2000 are not included.

I. DESIGNATED FOREIGN TERRORIST ORGANIZATIONS

1. **Abu Nidal Organization (ANO)**
2. **Abu Sayyaf Group (ASG)**
3. **Armed Islamic Group (GIA)**
4. **Aum Shinrikyo (Aum)**
5. **Basque Fatherland and Liberty (ETA)**
6. **Al-Gama'a al-Islamiyya (Islamic Group, IG)**
7. **HAMAS (Islamic Resistance Movement)**
8. **Harakat ul-Mujahidin (HUM)**
9. **Hizballah (Party of God)**
10. **Islamic Movement of Uzbekistan (IMU)**
11. **al-Jihad (Egyptian Islamic Jihad)**
12. **Kahane Chai (Kach)**
13. **Kurdistan Workers' Party (PKK)**
14. **Liberation Tigers of Tamil Eelam (LTTE)**
15. **Mujahedin-e Khalq Organization (MEK)**
16. **National Liberation Army (ELN) — Colombia**
17. **Palestine Islamic Jihad (PIJ)**
18. **Palestine Liberation Front (PLF)**
19. **Popular Front for the Liberation of Palestine (PFLP)**

20. PFLP-General Command (PFLP-GC)

21. al-Qa'ida

22. Real IRA (RIRA)

23. Revolutionary Armed Forces of Colombia (FARC)

24. Revolutionary Nuclei (formerly ELA)

25. Revolutionary Organization 17 November (17 November)

26. Revolutionary People's Liberation Army/Front (DHKP/C)

27. Shining Path (Sendero Luminoso, SL)

28. United Self-Defense Forces/Group of Colombia (AUC-Autodefensas Unidas de Colombia)

Legal Criteria for Designation

1. *The organization must be foreign.*
2. *The organization must engage in terrorist activity as defined in Section 212(a)(3)(B) of the Immigration and Nationality Act.*
3. *The organization's activities must threaten the security of U.S. nationals or the national security (national defense, foreign relations, or the economic interests) of the United States.*

II. OTHER TERRORIST GROUPS

Alex Boncayao Brigade (ABB)

Army for the Liberation of Rwanda (ALIR)

Continuity Irish Republican Army (CIRA)

First of October Antifascist Resistance Group (GRAPO)

Irish Republican Army (IRA)

Jaish-e-Mohammed (JEM) (Army of Mohammed)

Lashkar-e-Tayyiba (LT) (Army of the Righteous)

Loyalist Volunteer Force (LVF)

New People's Army (NPA)

Orange Volunteers (OV)

People Against Gangsterism and Drugs (PAGAD)

Red Hand Defenders (RHD)

Revolutionary United Front (RUF)

Source: "Patterns of Global Terrorism 2000" annual report, "Foreign Terrorist Organizations" (FTOs) 2001 biennial report, Office of the Coordinator for Counterterrorism, U.S. Department of State.

Terrorism: Threat Assessment, Countermeasures and Policy
ARTICLE ALERT

Cotter, Michael W. TRACKING DOWN THE TERRORISTS: REGIONAL ALLIES HAVE THEIR OWN AXES TO GRIND (*American Diplomacy*, vol. 6, no. 4, Fall 2001, http://www.unc.edu/depts/diplomat/articles/cotter_track/cotter_track.html)

The author, a former Ambassador in Turkmenistan, discusses various issues surrounding the tentative anti-terrorism coalition formed in the aftermath of the terrorist attacks on September 11th. He notes that many of Afghanistan's Central Asian neighbors (among them Israel, Russia, Iran, India, and Kyrgyzstan) have pledged some degree of support for the United States and the coalition, but he calls into question their motives for the move. He suggests that the many hidden agendas among the allies of the United States may make "tracking down the terrorists" a complex task. Cotter explains that strong and sustained political leadership as well as an organized and focused policy of diplomacy will be required in order to maintain a cohesive and cooperative coalition.

Jones, Curtis F. TERRORISM: ITS CAUSE AND CURE (*American Diplomacy*, vol. 6, no. 4, Fall 2001, http://www.unc.edu/depts/diplomat/articles/jones_terrorism/jones__terrorism.html)

Jones, a career diplomat, suggests that the United States is culpable in the provocation of terrorist acts because of the country's preoccupation with furthering national interests through its foreign policy. He argues that the United States must strive to find a balance between its national interest on the one hand, and morality and consensus of the international community on the other. Jones defines terrorism as "a necessary evil," in that it is a vehicle to express injustice, however, he goes on to explain the necessity of curbing terrorist activity by addressing basic human needs and grievances, rather than "answering bombs with bombs." He stresses the focus should be placed upon the reduction of political violence.

Weiss, Aaron WHEN TERROR STRIKES, WHO SHOULD RESPOND? (*Parameters*, vol. 31, no. 3, Autumn 2001, pp. 117-133)

In this article the author assesses the best respondent to terrorist attacks against America. The U.S. military's organization, discipline and mission-oriented culture have traditionally made it the first choice for policymakers seeking immediate action in a crisis. However, over dependency upon the military in a terrorist attack could decrease the military's ability to perform its primary warfighting role and, thus, increase the terrorist threat to the United States. Weiss views local agencies as the better respondents to a terrorist attack, supplemented with good planning, training and equipment. In light of the September 11th terrorist attack on America, the author's views are timely as counterterrorism policies, structures and appropriations are enacted.

Laqueur, Walter POSTMODERN TERRORISM (*Foreign Affairs*, vol. 75, no. 5, September/October 1996, http://www.foreignaffairs.org/Search/document_briefings.asp?i=19960901FAEssay4222.xml)

Historian Walter Laqueur believes the contemporary environment offers a bewildering multiplicity of terrorists and potentially terrorist groups and sects. Until now, terrorists were largely nationalists and anarchists, as well as extremists of the left and right. But in the current age, Laqueur says terrorism has found new inspiration for the users of pure violence. He says that history indicates that terrorism more often than not has little political impact, and that when it has an effect it is often the opposite of the one desired. He notes that 99 out of 100 terrorist attempts are likely to fail, but "the single successful one could claim many more victims, do more material damage, and unleash far greater panic than anything the world has yet experienced."

Pipes, Daniel WAR, NOT 'CRIMES' (*National Review* vol. LIII, no. 19, October 1, 2001, pg. 12)

Daniel Pipes argues that "[t]he time has come for a paradigm shift, toward viewing terrorism as a form of warfare." The consequences, which should follow from such a shift, Pipes writes, include targeting organizations and governments, which stand behind terrorists, and "relying on the armed forces, not policemen, to protect Americans." The United States, Pipes asserts, must establish a reputation for "certain and nasty" retribution against any terrorists who target Americans.

The annotations above are part of a more comprehensive Article Alert offered on the International Home Page of the Office of International Information Programs, U.S. Department of State: "http://usinfo.state.gov/admin/001/wwwhapub.html."

Terrorism: Threat Assessment, Countermeasures and Policy
BIBLIOGRAPHY

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (The Gilmore Commission). TOWARD A NATIONAL STRATEGY FOR COMBATING TERRORISM. Santa Monica, CA: Rand, December 15, 2000. 191p.

Alexander, Yonah; Swetnam, Michael S. USAMA BIN LADEN'S AL-QAIDA: PROFILE OF A TERRORIST NETWORK. Ardsley, NY: Transnational, 2001. 160p.

Badolato, Ed. HOW TO COMBAT TERRORISM (*The World & I*, vol. 16, no. 8, August 2001, pp. 50-53)

Cameron, Gavin; Pate, Jason; Vogel, Kathleen. PLANTING FEAR (*Bulletin of the Atomic Scientists*, vol. 57, no. 5, September/October 2001, pp. 38-44)

Combs, Cindy C.; Slann, Martin. ENCYCLOPEDIA OF TERRORISM. New York: Facts on File, 2001. 368p.

Cordesman, Anthony. TERRORISM, ASYMMETRIC WARFARE, AND WEAPONS OF MASS DESTRUCTION: DEFENDING THE U.S. HOMELAND. Westport, CT: Praeger, 2001. 456p.

Crenshaw, Martha. COUNTERTERRORISM POLICY AND THE POLITICAL PROCESS (*Studies in Conflict and Terrorism*, vol. 24, no. 5, September 2001, pp. 329-337)

Dempsey, James X. COUNTERTERRORISM AND THE CONSTITUTION (*Current History*, vol. 99, no. 636, April 2000, pp. 164-168)

Juergensmeyer, Mark. TERROR IN THE MIND OF GOD: THE GLOBAL RISE OF RELIGIOUS VIOLENCE. Berkeley: University of California, 2000. 332p.

Kozlow, Christopher. COUNTER TERRORISM. Alexandria, VA: Jane's Information Group, 2000. 285p.

Lesser, Ian O. COUNTERING THE NEW TERRORISM. Santa Monica, CA: Rand, 1999. 176p.

Parachini, John. NON-PROLIFERATION POLICY AND THE WAR ON TERRORISM (*Arms Control Today*, vol. 31, no. 8, October 2001, pp. 13-15)

Perl, Raphael. TERRORISM, THE FUTURE, AND U.S. FOREIGN POLICY. Washington: Congressional Research Service, Library of Congress, October 16, 2001. 16p.

Pillar, Paul R. TERRORISM AND U.S. FOREIGN POLICY. Washington: Brookings Institution, 2001. 272p.

Rashid, Ahmed. TALIBAN: MILITANT ISLAM, OIL, AND FUNDAMENTALISM IN CENTRAL ASIA. New Haven, CT: Yale University, 2001. 288p.

Stern, Jessica. THE ULTIMATE TERRORISTS. Cambridge, MA: Harvard University, 1999. 214p.

U.S. Congress, Senate, Committee on Foreign Relations. STRATEGIES FOR HOMELAND DEFENSE: A COMPILATION. Washington: Government Printing Office, September 26, 2001. 114p.

U.S. Department of Justice, Federal Bureau of Investigation. TERRORISM IN THE UNITED STATES. Washington: Government Printing Office, 2000. 68p.

U.S. Department of State, Counterterrorism Office. PATTERNS OF GLOBAL TERRORISM. Washington: Government Printing Office, April 2001. 81p.

U.S. General Accounting Office. COMBATING TERRORISM: SELECTED CHALLENGES AND RELATED RECOMMENDATIONS. Washington: Government Printing Office, September 2001. 218p.

U.S. General Accounting Office. CRITICAL INFRASTRUCTURE PROTECTION. Washington: Government Printing Office, April 2001. 108p.

U.S. Government. CONPLAN: INTERAGENCY DOMESTIC TERRORISM CONCEPT OF OPERATIONS PLAN. Washington: Government Printing Office, January 2001. 43p.

U.S. National Commission on Terrorism. COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM. Washington: Government Printing Office, June 2000. 44p.

Terrorism: Threat Assessment, Countermeasures and Policy
KEY INTERNET SITES

Please note that the U.S. Department of State assumes no responsibility for the content and availability of the resources listed below; such responsibility resides solely with the providers.

Center for Defense Information: Terrorism Project
http://www.cdi.org/terrorism/

Center for Nonproliferation Studies: Terrorism
http://cns.miis.edu/research/terror.htm

Center for Strategic and International Studies: Homeland Defense
http://www.csis.org/burke/hd/index.htm

The Centre for the Study of Terrorism and Political Violence
http://www.st-and.ac.uk/academic/intrel/research/cstpv/

Council on Foreign Relations: Terrorism Resource Center
http://www.cfr.org/Public/media/attack.html

The Counter-Terrorism Page
http://www.terrorism.net/home.asp

The Henry L. Stimson Center: Chemical and Biological Terrorism
http://www.stimson.org/cwc/terror.htm

The International Policy Institute for Counter-Terrorism
http://www.ict.org.il/institute/ict.htm

National Security Institute: Counter Terrorism
http://nsi.org/terrorism.html

Studies in Conflict and Terrorism
http://www.tandf.co.uk/journals/tf/1057610X.html

Terrorism and Political Violence
http://www.frankcass.com/jnls/tpv.htm

Terrorism Research Center
http://www.terrorism.com/index.shtml

U.S. Centers for Disease Control and Prevention: Bioterrorism Preparedness and Response
http://www.bt.cdc.gov/

U.S. Central Intelligence Agency: The War on Terrorism
http://www.odci.gov/terrorism/index.html

U.S. Critical Infrastructure Assurance Office
http://www.ciao.gov/

U.S. Department of State: Bureau of Diplomatic Security: Overseas Security Advisory Council
http://www.ds-osac.org/

U.S. Department of State: Counterterrorism Office
http://www.state.gov/s/ct/

U.S. Department of State: Diplomatic Security Service: Rewards for Justice
http://www.dssrewards.net/

U.S. Department of State: Foreign Terrorist Organizations
http://www.state.gov/s/ct/rls/rpt/fto/

U.S. Department of State: International Security: Response to Terrorism
http://usinfo.state.gov/topical/pol/terror/

U.S. Environmental Protection Agency: Counter-Terrorism
http://www.epa.gov/swercepp/cntr-ter.html

U.S. Federal Bureau of Investigation: National Infrastructure Protection Center
http://www.nipc.gov/

U.S. Federal Emergency Management Agency: Fact Sheet: Terrorism
http://www.fema.gov/library/terror.htm

U.S. Mission to the U.N.: Political and Security Affairs: Terrorism
http://www.un.int/usa/terror.htm

U.S. FOREIGN POLICY
AGENDA

VOLUME 6 AN ELECTRONIC JOURNAL OF THE U.S. DEPARTMENT OF STATE NUMBER 3

Threat Assessment, Countermeasures and Policy

November 2001